71. (New) A method for enabling strong mutual authentication on a computer network comprising the steps of:

transmitting, by a server computer, a first encrypted message to a client computer over a first communication channel;

receiving, by said client computer, a key over a second communication channel; and

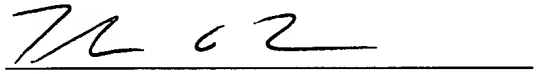
transmitting, by said client computer, a decrypted message over said first communication channel.

REMARKS

This preliminary amendment adds new claims 49-71. The new claims add no new matter and are supported throughout the specification and figures. Claims 1-71 are now pending.

If the Examiner believes that a telephone conversation with Applicants' attorney would be helpful in expediting prosecution of the application, the Examiner is invited to call the undersigned at (617) 248-7738.

Respectfully submitted,



Date: October 24, 2001
Reg. No. 35,722

Thomas A. Turano
Agent for Applicants
Testa, Hurwitz, & Thibeault
High Street Tower
125 High Street
Boston, Massachusetts 02110

Tel. No. (617) 248-7738
Fax: (617) 248-7100

MARKED-UP COPY OF AMENDMENTS TO THE CLAIMS

17. (Amended) A ~~The~~ method for authenticating a third device to a first device comprising the steps of:

encrypting a first key with a second key by said first device;

encrypting said second key with a third key by said first device;

decrypting said encrypted second key in response to said third key by a second device; and

decrypting by said third device said encrypted first key using said second key obtained from said second device.

21. (Amended) A ~~The~~ method for authenticating a third device to a first device comprising the steps of:

transmitting by said first device a first message to said third device;

transmitting by said first device a second message to a second device;

transmitting by said second device a second key of said second message to said third device; and

obtaining by said third device a first key of said first message using said second key of said second encrypted key.

49. (New) A method for enabling strong mutual authentication on a computer network comprising the steps of:

transmitting, by a first computer, a first encrypted message to a second computer over a first communication channel; and

transmitting, by said first computer, a second message to said second computer over a second communication channel, wherein said second message comprises a second authentication number to decrypt said first message.

50. (New) The method of claim 49, wherein said first message comprises a first authentication number.

51. (New) The method of claim 50, wherein said first authentication number is encrypted by said second authentication number.

52. (New) The method of claim 49 further comprising transmitting a first indicia to said first computer over said first communication channel.

53. (New) The method of claim 49 further comprising generating, by said first computer, at least one of said first authentication number and said second authentication number.

54. (New) The method of claim 49 further comprising generating, by said first computer, a third authentication number.

55. (New) The method of claim 49 further comprising transmitting, by said first computer, said second message to a verifier over said second communication channel and transmitting by said verifier said second message to said second computer over said second communication channel, wherein said second message comprises said second authentication number encrypted.

56. (New) The method of claim 49, wherein said second communication channel further comprises a third communication channel.

57. (New) The method of claim 49, wherein said second message further comprises a third authentication number.

58. (New) The method of claim 55 further comprising decrypting, by said verifier, said second message to obtain a first decrypted message, wherein said first decrypted message comprises said second authentication number.

59. (New) The method of claim 55, wherein said transmitting said second message to said second computer over said second communication channel further comprises transmitting, by said verifier, said second authentication number to said second computer over said second communication channel.

60. (New) The method of claim 49 further comprising decrypting, by said second computer, said first message transmitted by said first computer to recover said first authentication number.

61. (New) The method of claim 49 further comprising transmitting, by said second computer, a third message to said first computer over said first communication channel, wherein said third message comprises said second authentication number encrypted by said first authentication number.

62. (New) The method of claim 50 further comprising validating said second computer by said first computer by decrypting said third message to obtain said second authentication number.

63. (New) The method of claim 49, wherein said second message further comprises an encrypted portion.

64. (New) A system for enabling strong mutual authentication comprising:

a first transmitter; and

a first receiver in communication with said first transmitter over a first communication channel and in communication with said first transmitter a second communication channel;

wherein said first transmitter transmits a first encrypted message to said first receiver over said first communication channel; and

wherein said first transmitter transmits a second message to said first receiver over said second communication channel to decrypt said first encrypted message.

65. (New) The system of claim 64 further comprising:

a second transmitter; and

a second receiver in communication with said second transmitter over said first communication channel;

wherein said second transmitter transmits a first indicia to said second receiver over said first communication channel,

wherein said second transmitter transmits a third message to said second receiver over said first communication channel, said third message comprising at least a portion of said decrypted first encrypted message.

66. (New) The system of claim 65 further comprising a comparator in communication with said first transmitter and said second receiver to compare at least a portion of said third message with at least a portion of said first encrypted message decrypted.

67. (New) The system of claim 64, wherein said second message is encrypted.

68. (New) The system of claim 67 further comprising a verifier in communication with said first transmitter to decrypt said encrypted second message to obtain a key to decrypt said first encrypted message.

69. (New) An apparatus for enabling strong mutual authentication on a computer network comprising:

means for transmitting a first message to a computer over a first communication channel, wherein said first message comprises a first encrypted authentication number; and

means for transmitting a second message to said computer over a second communication channel, wherein said second message comprises a second authentication number to decrypt said first message.

70. (New) The apparatus of claim 69 wherein said first encrypted authentication number is encrypted by said second authentication number.

71. (New) A method for enabling strong mutual authentication on a computer network comprising the steps of:

transmitting, by a server computer, a first encrypted message to a client computer over a first communication channel;

receiving, by said client computer, a key over a second communication channel; and

transmitting, by said client computer, a decrypted message over said first communication channel.